STATEMENT OF ARGUMENTS

The following listing of clear errors is responsive to the Office Action mailed November 19, 2019, and the Advisory Action mailed March 24, 2010, each of which errors independently should result in reversal and withdrawal of all of the rejections.

CLAIMS 2-6, 8 AND 16-18 COMPLY WITH THE WRITTEN DESCRIPTION REQUIREMENT UNDER 35 U.S.C. §112, FIRST PARAGRAPH

The Examiner stated that the limitation "the gateway including notification means for initiating an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that it should initiate a secure authenticated connection with the gateway when the notification means is requested so to do by any one of the services offered by the first sub-system" of claim 16, and the limitation "initiating from the notification means to the application hosting sub-system an unauthenticated and unencrypted connection and transmitting over this connection the notification for notifying said application hosting sub-system that it should initiate a secure authenticated connection with the gateway" of claim 17, do not have support in the instant specification, see p. 4 of the Office Action of 11/19/2009.

Section p. 11, lines 13-16 of the instant specification recites "As a result of the processing performed by notification server 220, the notification server 220 initiates a simple (unauthenticated and unencrypted) TCP/IP connection 450 with listener 112 and transmits over this connection a notification (the nature of which will be described in greater detail below) to listener 112". This section teaches that the notification means sets up an unauthenticated and unencrypted connection and then it transmits a notification message over this connection.

Moreover, p. 11, lines 18-22, of the instant specification ("Upon receipt of the notification, listener 112 forwards this notification via forward notification communication 455 to a notification processing module (not shown) within the main (client application specific) part 11 of the application 110 which processes the notification and thereby establishes that it should attempt to contact the SMS service plug-in 257"), teaches that the notification is sent as a result of being requested to do so by any of the services (e.g., the SMS service 257).

In view of the above-noted portions (pg. 11, lines 13-16 and 18-22) in the instant specification, the above-noted claim limitations are supported by the instant specification.

In response to the above arguments, the Examiner stated that "the claimed application hosting sub-system and the listener 112 in the supported portion are interpreted as not being

connected or related. There is not any definition that describes the claimed application hosting sub-system is the listener 112", see Advisory Action of 3/14/2010.

As it can be seen in Fig. 2 of the instant specification, the listener 112 is part of the client application hosting sub-system 110. Box 112 is within the confines of the application hosting sub-system, and it is not shown by itself or within the gateway 200 or within the mobile operator 300. Moreover, the above mentioned section p. 1, lines 18-22 of the specification infers that the listener 112 is part of the application hosting sub-system, receives the notification, and transmits it to the notification processing module of the application hosting sub-system.

For the above reasons, independent claims 16 and 17 have support in the instant specification. Dependent claims 2-6, 8 and 18 also fully comply with 35 U.S.C. §112, first paragraph.

INDEPENDENT CLAIMS 16 AND 17 ARE NOT OBVIOUS OVER GRANTGES, JR. ET AL. (US 6,510,464) IN VIEW OF WILDING (US 2005/0050329)

None of the prior art teaches or suggests "the *gateway* including notification means for *initiating* an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems and transmitting over this or each such connection a notification for notifying said one or more of the application hosting sub-systems that *it should initiate a secure authenticated connection with the gateway when the notification means is requested so to do by any one of the services offered by the first sub-system*", emphasis added, as required by claim 16 (similarly for claim 17).

The Examiner acknowledged that Grantges does not disclose the above feature and turned to Wilding for the missing limitation, see p. 6 of the Office Action of 11/29/2009.

Wilding discloses a method such that a customer system 102 can establish a secure connection with an organization system 104 using a public network, allowing the customer system 102 to communicate with the organization system 104 in a secure manner, while authenticating the identity of the customer system 102 to the organization system 104 and vice versa (Fig. 1). According to the method, once the customer has registered with the server, the customer system initiates a connection, [0028]. A temporary Server Public Key is sent from the service gateway to the customer system using the TCP connection initiated by the customer system. A series of encryption packages is sent back and forth between the gateway and the customer system over this TCP connection initiated by the customer system, until a remote, secure authenticated and encrypted connection has been established between the service client 108 and the service gateway 110.

The Examiner asserted that the process "starting from the step of transmitting the Temporary Server Public Key from the service gateway 110 to the service client 108 (i.e., interpreted as a notification to verify the authenticated information); until the step of establishing secure, authenticated and encrypted connection between the service gateway 110 and the service client 108" disclosed by Wilding reads on the above missing limitation, see p. 6 of the Office Action of 11/29/2009.

The Examiner's assertion is not true. In Wilding, it is clear from paragraph [0028] ("Once the customer has registered with the server, a remote service session can be established. Referring to FIGS. 3A-3B, a flow chart illustrating the steps for establishing a remote session is shown. In step 302, the customer system initiates a connection. The service client 108 establishes a Transmission Control Protocol/Internet Protocol (TCP/IP) connection, or session, to the service gateway 110. This is similar to having the customer use the telnet protocol to connect to a remote system through the Internet, although the following steps ensure a much higher level of security than a telnet connection"), emphasis added, that the connection is initiated by the customer system. All the encryption packages being sent back and forth between the customer and the service gateway are sent over the TCP connection initiated by the customer system.

In contrast, claim 16 requires "the *gateway including notification means for initiating* an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems". In other words, in the invention of claim 16, it is the gateway that initiates an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems, for the purpose of asking the one or more application hosting sub-systems to initiate a secure connection with the gateway, not the one or more of the application hosting sub-systems.

In addition, regarding Grantges, the Examiner identified an "options page" being sent by gateway web server 44 in a message 78 to client computer 22 (Fig. 2), the "options page" presenting a list of authorized applications 24_1, 24_2...24_3 for selection by user 18 of client computer 22, as the claimed "when the notification means is requested so to do by any one of the services offered by the first sub-system", see p. 6 of the Office Action.

However, even assuming *arguendo* (which Applicant does not believe to be the case) that message 78 including an "options page" corresponds to "notification means", this cannot be interpreted as it being requested by any one of the services offered by the first sub-system (identified as the applications 24_1, 24_2...24_3 by the Examiner), as required by claim 16. Instead, in Grantges, the notification is requested by the user 18 (which was identified by the Examiner as the claimed application hosting sub-system). Message 74 is not generated in response to a request from the any one of the Applications (App. 1, App. 2, App.3) of Grantges, but in

response to a request issued from the DMZ proxy server 34 which itself was initiated as a result of receiving a request from the web browser 22 for connection to the system 20 as a whole. In addition, an options page presented to the client computer 22 merely represents what is available to the client computer, not a specific request by one of the services offered by the first sub-system to the client computer to initiate a secure authenticated connection with the gateway.

It is clear in Grantges, e.g., col. 8, lines 18-20 ("User 18, via client computer 22, through its web browser, initiates a request 64 for authentication…"), that the connection is initiated by the user. Thereafter, information is passed back and forth using the connection, but it is not initiated by the web server 44 (corresponding to the claimed gateway including notification means), as required by claim 16 ("the *gateway including notification means for initiating* an unauthenticated and unencrypted connection to one or more of the application hosting sub-systems" , emphasis is added).

One of ordinary skill in the art would not have looked into modifying Grantges in order to include notification means. In Grantges, there is no perceived need for notifications to be sent to the users 18. This is because the services provided by applications 1, 2 and 3 are conventional services adhering to a classic client/server model where servers simply respond to an input request from a client. The only mention of applications in Grantges (col. 5, lines 24-30) does not suggest that they might ever need to send a notification to a user to contact the server, nor accordingly is there any discussion of any mechanism for sending such notifications.

For the above reasons, claim 16 is allowable. Claim 17 includes limitations similar to those of claim 16 and is also allowable.

It is respectfully requested that the rejection of claims 2-6, 8 and 18, all dependent form claim 16 or 17, also be withdrawn.